UNIVERSITY OF CALIFORNIA

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

THE PRIVACY RULE

----------------------

PHI REFERENCE MANUAL

for the training module

“PHI MANAGEMENT FOR DATA STEWARDS”

(Abbreviated Title: “PHI Reference Manual”)

Issued: March 31, 2003
Introduction
This manual has been prepared to assist “PHI Data Stewards” – those individuals who disclose or provide access to Protected Health Information (PHI) as part of their job function, or interact with patients regarding their health information requests or questions.

Data stewards:
1. Receive and review requests for PHI;
2. Provide access to and disclose PHI as allowed by HIPAA and other state and federal laws;
3. Prevent access to or disclosure of PHI except as permitted or allowed by law; and
4. Serve as the University’s liaison to the patient when the patient wants to exercise his/her HIPAA Privacy Rights.

Examples of PHI Data Stewards
Health Information Management Services (HIMS) / Medical Records staff, medical billing office / patient accounting staff, Clinic/emergency staff, Admissions & Registration staff, Pharmacy staff, Health Plan staff, Hospital Unit staff, Lab / Radiology staff, Physical / Occupational Rehabilitation service staff, Case managers / Utilization review staff, Information Technology services staff, Research staff, Patient assistance / relations staff, Risk Management staff, Home Health staff and others identified as having by access to protected health information (PHI) as part of their job duties/title..

Objectives
The PHI Management Training Module provides specific training on HIPAA and responsibilities of data stewards for complying with the federal requirements for using and disclosing PHI. This Reference Manual should be used in combination with the PHI Management Module. The HIPAA Privacy Rule is complex and will require all workforce members to change the way that they handle health information. Because data stewards receive requests for PHI from workforce members (for example, physicians, researchers, faculty, auditors, attorneys, trainees), it is very important that data stewards understand the specific requirements of HIPAA and University policy. Data stewards may also receive requests from patients and their family members, outside third parties, University contractors, members of law enforcement, judicial or governmental entities. Your job as a PHI Data Steward is very important in protecting health information and ensuring compliance with the HIPAA Privacy Rule requirements. However, you are not alone, and if at any time you need assistance in handling a request, you can contact: your supervisor, the campus Privacy Officer or Legal Counsel, the University’s Privacy Official and UC General Counsel.

Resources
The University of California has also developed a number of resources to assist all workforce members in achieving compliance with the HIPAA Privacy Rule:

1. The University’s Systemwide HIPAA Standards and Implementation Policies
2. The University’s approved legal documents and forms:
   a. Notice of Privacy Practices (NPP) and Acknowledgement form
   b. Authorization Forms
   c. Business Associate Agreement (BAA)
   d. Power Point Training Modules
3. Campus HIPAA Policies and Procedures
4. University HIPAA Privacy WebSite
## Crosswalk: “PHI Management for Data Stewards” Module and “PHI Reference Manual”

<table>
<thead>
<tr>
<th>CONTENTS</th>
<th>PHI REFERENCE MANUAL</th>
<th>PHI Module POWER POINT SLIDE NUMBERS</th>
<th>UNIVERSITY HIPAA STANDARDS NUMBER (Std. #)</th>
<th>CAMPUS POLICY &amp; PROCEDURES NUMBER (if applicable)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Patient’s Privacy Rights under HIPAA</td>
<td>2, 7, 8</td>
<td>11, 12, 17-24, 51-53, 54-64</td>
<td>Std. 4, 11, 12</td>
<td></td>
</tr>
<tr>
<td>2. Access to PHI by Health Care Provider Team</td>
<td>1, 4, 5</td>
<td>11-15, 25-35, 70</td>
<td>Std. 1</td>
<td></td>
</tr>
<tr>
<td>3. Access to PHI by Other Members of the Workforce</td>
<td>1, 4, 5</td>
<td>25-36</td>
<td>Std. 1</td>
<td></td>
</tr>
<tr>
<td>4. Access to PHI by Business Associates</td>
<td>1, 14</td>
<td>35</td>
<td>Std. 17</td>
<td></td>
</tr>
<tr>
<td>5. Access to PHI by Health Professional Training Programs Faculty and Trainees</td>
<td>1, 10</td>
<td>32-34</td>
<td>Std. 7</td>
<td></td>
</tr>
<tr>
<td>6. Access to PHI by University Researchers</td>
<td>9, 10</td>
<td>40-42, 47-50</td>
<td>Std. 2, 9</td>
<td></td>
</tr>
<tr>
<td>7. Access to PHI by Third Parties When the Patient has the Opportunity to Object</td>
<td>2, 3</td>
<td>36-39, 55-56, 21, 22, 17-23</td>
<td>Std. 4, 11, 12</td>
<td></td>
</tr>
<tr>
<td>a. Facility Directory</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>b. Family and Friends</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c. Personal Representative</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Access to PHI by Third Parties when the Patient has the opportunity to object or provide an Authorization</td>
<td>6, 12</td>
<td>11, 36-39</td>
<td>Std. 6, 10</td>
<td></td>
</tr>
<tr>
<td>9. Access to PHI by Third Parties when the Patient does not have the opportunity to object or provide Authorization</td>
<td>6</td>
<td>11, 43-50</td>
<td>Std. 7, 8, 9</td>
<td></td>
</tr>
<tr>
<td><strong>Appendix</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Notice of Privacy Practices (NPP) - weblink</td>
<td></td>
<td>70-71</td>
<td>Std. 4</td>
<td></td>
</tr>
<tr>
<td>B. Sample Authorization Form – weblink</td>
<td></td>
<td>70-71</td>
<td>Std. 6</td>
<td></td>
</tr>
<tr>
<td>C. Sample Business Associate Agreement – weblink</td>
<td></td>
<td>70-71</td>
<td>Std. 17</td>
<td></td>
</tr>
<tr>
<td>D. Sample Data Use Agreement – weblink</td>
<td></td>
<td>70-71</td>
<td>Std. 2</td>
<td></td>
</tr>
<tr>
<td>E. Definitions of HIPAA Terms – weblink (full defs.)</td>
<td></td>
<td>71</td>
<td></td>
<td></td>
</tr>
<tr>
<td>F. Other references / weblinks</td>
<td></td>
<td>71</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
List of Policy Summary Sheet Numbers and HIPAA Fact Sheets included in this Reference Manual

1. Confidentiality of Protected Health Information (PHI)
2. Provision of the “Notice of Privacy Practices” (NPP)
3. Information, Disclosure of Patient Facility Directory to the Public and Media
4. Facsimile (Faxing) of Protected Health Information (PHI)
5. Health Information: Access, Use and Disclosure of PHI
6. Health Information: Disclosure of PHI for Law Enforcement
7. Health Information: Request for an Accounting for Disclosures of PHI
8. Health Information: Request for an Amendment or Addendum of PHI
9. Research: Access, Use and Disclosure of PHI
10. De-Identifying and Re-Identifying Data that Contains PHI; Limited Data Sets; Data Use Agreements
11. Fact Sheet: De-Identified Data vs. Limited Data Sets (LDS)
12. Uses & Disclosures of PHI for Fundraising / External Relations, Media / Public Information, Marketing
13. Personal Representatives
14. Fact Sheet: Business Associates
15. Fact Sheet: Reasonable Copy Fees
16. Fact Sheet: Security Standards
17. Fact Sheet: Standards for Electronic Transaction & Code Sets

List of Common HIPAA Abbreviations and Key Concepts

BA – Business Associate
BAA – Business Associate Agreement
CE – Covered Entity
DDS – De-identified Data Set, Data that has been stripped of the 18 PHI identifiers
DRS – Designated Record Set
DUA - Data Use Agreement
HIMS – Health Information Management Services (medical records)
HIPAA – Health Insurance Portability & Accountability Act of 1996, Privacy Rule
IRB – Institutional Review Board (for human research)
LDS – Limited data set for health care operations, public health, teaching and research purposes only
MNS – Minimum Necessary Standard, “need to know”
NPP – Notice of Privacy Practices
OCR – Office for Civil Rights
PHI – Protected Health Information
PO – Privacy Officer
PR -- Personal Representative
TPO – Treatment, Payment, Operations
UC – University of California Health System
U&D – Uses & Disclosures

Refer to Appendix _E_ for a complete listing of HIPAA definitions from the Privacy Rule.
HIPAA PRIVACY - POLICY SUMMARY - #1

Title: Confidentiality of Protected Health Information (PHI)

SUMMARY
This policy describes the legal and ethical responsibility for the protection of the privacy and confidentiality of patient’s protected health information (PHI). The policy establishes responsibilities and safeguards that all personnel are responsible and accountable for following. In addition, sanctions for the misuse and inappropriate access of protected health information are described in the policy. The expectation to protect health information applies to everybody that has access to the healthcare environment, whether an employee, physician, volunteer, student, intern or contractor. Your signature on the Confidentiality and Non Disclosure Agreement establishes your commitment and obligation to the protection of information.

CRITICAL EDUCATION POINTS

Our Responsibilities
- To protect the health information that identifies a patient, is created or obtained in the process of caring for the patient, and is kept, filed, used or shared in an oral, written or electronic format.
- To review the privacy education training materials (modules) and UC “Notice of Privacy Practices”
- Determine and apply appropriate safeguards for protection of information in consideration of patient care needs and safety.
- Report suspected violations of privacy and confidentiality

Minimum Necessary, Need to Know: Only access information needed to do your job. You are not allowed to view or obtain information about you, your co-workers, family, or friends.

Unauthorized Access: Accessing or communicating confidential information not associated with your job responsibility is considered a violation of this policy and will result in corrective action which may include termination of your relationship with the organization and also have personal legal consequences.

Apply Standard Safeguards
- Know the additional privacy practices and policies specific to your department.
- Protect confidential information from unauthorized access, use or disclosure.
- Maintain physical security, access control, locked storage as appropriate, i.e., keep doors closed to secure areas, obey posted signs for restricted access to secure areas.
- Notify a clinical staff member if medical records are left unattended in public view.
- Never dispose of paper or items containing patient information in the regular trash.
- Confidential information should never be discussed in public areas, such as hallways, cafeterias, or restrooms.
- Report known or suspected violations of privacy.
- Computer passwords are unique, do not share your password or log on a computer for someone else.
- Stop and question individuals who do not belong in your work area.
- Never remove paper or items containing patient information from the facility unless authorized to do so.

Reporting privacy concerns and suspected violations, leads to improved practices and further fosters a culture of respect for our patients. Each of us has an obligation to report suspected violations and concerns. Report concerns to the charge nurse, your supervisor or the UC_HS Privacy Officer.
Title: Provision of the “Notice of Privacy Practices” (NPP)

SUMMARY
Each hospital / facility will give all patients accessing health services a Notice of Privacy Practices. The Notice informs individuals of the permitted uses and disclosure that may be made of their health information, the individual’s rights regarding his/her information and the responsibilities to protect health information. The federal privacy regulations mandate elements that must be included in a Notice. All personnel should read the Notice, know their responsibility for protecting information and be able to direct individuals who have questions or complaints regarding privacy practices to the appropriate resource.

CRITICAL EDUCATION POINTS

Right to a Notice of Privacy Practices (NPP)
The Notice of Privacy Practices serves to inform patients or their legal representatives of:
- Ways we may use and disclose protected health information (PHI)
- The patient’s rights regarding their health information
- Legal responsibilities with respect to PHI
- There are two University of California Notices – medical services (NPP-Medical) and a separate notice for mental health services (NPP-MH)
  Required Notice elements may be found in 45 CFR 164.520, California requires a 12-point font.

- Notice must be provided at the time of “1st” service delivery
  - Patients must be provided with the NPP at least once after 4/14/03, at the first service delivery
  - In emergency treatment, the notice must be provided as soon as reasonably practical
  - The Notice may be furnished personally or sent by electronic mail, or mail or fax if the patient authorizes
  - The Notice will be posted in service areas and on the Health care provider’s web site

- Acknowledgement of Receipt of the Notice
  - A good faith effort must be made to obtain written Acknowledgement from the patient or his/her legal representative that they received the Notice
  - If patient refuses to sign or is unavailable to sign (e.g., left before signature could be obtained), document reasons why the Acknowledgment was not signed
  - Signed Acknowledgments are retained for 6 years according to each facility’s procedures, e.g., file in the medical record, EDI, or SV3 for scanning

OPPORTUNITY TO OBJECT

- Inform Patients of the “Inpatient / Facility Directory”
  - Patient Directory includes only name, location in facility, one-word condition description and, to verified members of the clergy, religious affiliation.
  - Patients may restrict all or part of their information in the directory, usually at the time of inpatient admission.

- Restriction of Information
  If patients request restrictions on their information beyond inclusion in the inpatient Facility Directory, notify a supervisor to speak to the patient. Accommodating further restrictions to patient information will be based on the scope and the reason for the request and each facility’s system capabilities to accommodate the requested restrictions.

- Requests for alternate "confidential communications"
  Patients may request that their information be communicated in alternate manner. An example may be that a patient requests that a bill be sent to an alternate address. Admissions / registration staff will accommodate reasonable requests.

- Patient questions and concerns regarding the NPP or Notice. Refer patients to your supervisor or the Privacy Officer.
HIPAA PRIVACY - POLICY SUMMARY - #3

Title: Information, Disclosure of Patient / Facility Directory to the Public and Media

SUMMARY

The privacy regulations allow the disclosure of certain information maintained in a "Patient / Facility Directory". The information contained in the directory is very limited. Patients are informed of the Patient / Facility Directory at each admission and have the opportunity to restrict entirely or limit information that may be disclosed. This policy provides guidance for the disclosure of Patient / Facility Directory information to family, friends, and the media who ask for the patient by name, and to clergy.

CRITICAL EDUCATION POINTS

Patient Directory
The University must maintain a directory of individuals currently in the facility. Exception: For further protection of privacy, behavioral health and alcohol treatment patients will never be included in the Patient Directory.
✓ Patients may choose to include or restrict all or part of their information in the inpatient facility directory.

Directory Information is limited and may only be released to individuals who inquire about the patient by name, information includes:
✓ Patient name
✓ Location (e.g., Emergency Department or Inpatient)
✓ Condition (one word), obtain from physician or appropriate clinical staff
  ✐ Undetermined: Patient is awaiting the physician and assessment
  ✐ Good: Vital signs are stable and within normal limits. Patient is conscious and comfortable. Indicators are excellent
  ✐ Fair: Vital signs stable, within limits. Patient is conscious but may be uncomfortable. Indicators are favorable.
  ✐ Serious: Vital signs may be unstable and not within normal limits. Patient is acutely ill, indicators are questionable.
  ✐ Critical: Vital signs are unstable and not within normal limits. Patient may be unconscious. Indicators are unfavorable.
✓ Religion (available only to clergy)

Patient Restrictions: If a patient’s request for restriction of his/her protected health information (PHI) is granted, the information may not be disclosed. The response to inquiries about a patient should be, "We do not show an individual by that name in our Patient Directory". If a caller is persistent, contact a supervisor for assistance. In cases in which the patient is unable to express/request restrictions (e.g., comatose / celebrity), use professional judgment or consult with the treating provider to determine whether to impose restrictions.

Media Requests for Information:
✓ Media requests for information regarding a specific patient. Patient Directory information may be provided to the media if they inquire about the patient by name. If the media do not have the patient name, no information will be disclosed.
✓ Marketing and Communications or an Operation Supervisor should be called to respond to all media requests.
✓ Media should always be escorted while in the facility. Ask media members to wait in the lobby while you call your supervisor or communications representative for an escort.
[Insert Facility Specific procedures]
Title: Facsimile (Faxing) of Protected Health Information (PHI)

**SUMMARY**

This policy provides staff with guidance on the appropriate use of facsimile (fax) transmission of information to ensure the confidentiality and security of information.

**CRITICAL EDUCATION POINTS**

**Utilization of Fax transmission** for communication of information will be determined using the following criteria:

- Fax transmission is the appropriate means of communication
- Sender's authority to disclose and the recipient's authority to receive information is verified
- Security status and protection requirements of information being transmitted are considered

**Protected Health Information (PHI) may be transmitted by fax when (examples):**

- Original record or mail delivered copies will not meet the immediate needs of patient care
- When PHI is urgently required by a third party payer and failure to facsimile the records could result in loss of reimbursement
- Pursuant to a patient/legal representative's authorization
- Upon request from a member of the patient’s healthcare provider team for treatment, payment or healthcare operations (TPO)

**Authorization to Disclose PHI:**

Assess the need for specific patient authorization to disclose the information prior to faxing.

**Limit information being faxed to the minimum necessary:**

Faxed information should always be limited to the amount necessary to achieve the purpose of the communication. Limit information to effectively facilitate safety, treatment, essential healthcare operations and continuity of care.

**Fax Safeguards:**

- Verify accuracy of fax numbers with intended recipient before sending a fax
- Use fax cover sheets
- **Notify facilities that you commonly receive faxes from if your number changes**
- Recipients you commonly fax numbers to should be pre-programmed
- When faxing PHI, verify fax number and availability of recipient prior to sending
- Locate machines out of public view
- Establish a routine for regular removing/distribution of incoming faxes

**Pre-programmed Fax Numbers:**

- Use pre-programmed numbers whenever possible
- Pre-program number and send test fax-requesting verification of receipt

**Fax Cover Sheet Requirements:**

- Completed cover sheets with standard confidentiality statement and disclaimer are required on all organizational fax transmissions of PHI.

**Exception:** Routing faxing of information from department to department within the building, using a pre programmed fax number may not require a fax cover sheet. See policy for details of requirements. [Facility specific policy]

**Misdirected faxes:** Obtain the fax number of the unintended receiver and immediately transmit a request that the material be destroyed immediately or retrieved by mail or delivery. If fax contained PHI, notify a supervisor, log the disclosure.
HIPAA PRIVACY - POLICY SUMMARY - #5

Title: Health Information: Access, Use and Disclosure of PHI

SUMMARY
To ensure the protection and confidentiality of protected health information in compliance with state and federal law, this policy describes the circumstances under which you may access, use and disclose protected health information as well as the authorizations required that may be required to use or disclose PHI.

CRITICAL EDUCATION POINTS
Staff authorized to disclose protected health information (PHI) should be familiar with all facility policies regarding the authorization and disclosure of information. Policy highlights include:

Access to PHI: Access to PHI is limited to those individuals:

- Providing care and treatment
- Requiring information for payment/billing activities
- Participating in functions of health care operations
- Other uses/disclosures of PHI authorized by law, as referred to in the NPP

Disclosure of PHI: Generally any disclosure made outside of the organization, not for the purpose of TPO, or mandated or permitted by laws, requires patient authorization. Always consider the circumstance information is being released under. If in doubt, consult with Health Information Department or obtain the patients authorization. Use the standard "Authorization for Use and Disclosure of Health Information" form found on all units and in the Health Information Department.

Use of PHI: The Privacy Regulations allow use and disclosure of a patient's protected health information without a patient authorization in the following circumstances:

- For providing Treatment, Payment and Health Care Operations (TPO): In order to carry out treatment, payment and healthcare operations, i.e., sharing information with other providers, transfer of patient to another facility, coordinating continuing care. Payment activities with third parties for the purpose of obtaining payment. Risk management, utilization review, fundraising, training/education and performance improvement activities in support of hospital operations.
- Mandated and required reporting: Staff will continue to disclose PHI as mandated or required under various state and federal regulations, i.e. abuse, assault, infectious disease, public health activities, organ and tissue donation.
- Individuals Involved in the patients care: Clinical staff may share relevant information with individuals who have been identified by the patient as being involved in their care.

HIV/AIDS test results, Psychiatric and Drug/Alcohol treatment Information, Genetic Testing always requires specific Patient Authorization for disclosure under all circumstances: These types of information are protected under additional regulations and may require a patient authorization for release. The attending physician must be consulted prior to release of any mental/behavioral health information to a patient.

Responding to requests for information: Whenever possible, Health Information personnel should process requests for information. If health information personnel are not available however, authorized personnel may disclose the information. It is critical that the policy and procedure is followed closely and the appropriate documentation form be completed and signed.

Verify Authority and Identity: When disclosing information, verify the authority of the individual requesting information, check identification by asking for ID or for telephone requests, ask for confirmation of authority, e.g., account number, and a second identifier or use a call back number to confirm access procedure.

Documentation of Disclosures: It is important that disclosures made outside of the organization for reasons other than TPO be documented. Complete the appropriate documentation form and ensure that it is included in the medical record or provided to the Health Information Department. This includes oral, written and electronic disclosures and disclosures made in error. Examples include, abuse / neglect required reporting, law enforcement.

Patient Access: Patients have a right to view or obtain copies of their health information. Refer the patient to the Health Information Management Services department whenever possible. There are circumstances when access to records may be denied. Clinicians responding to patients requests for access to their information should be familiar with the circumstances in which access should be denied. For patients requesting to view their open medical record, a physician order is required. An appropriate clinician should review the information with the patient.
**Title:** Health Information: Disclosure of PHI to Law Enforcement

**SUMMARY**

The Privacy Regulations allow the disclosure of certain protected health information (PHI) to law enforcement officials without the authorization of the patient. This policy describes the circumstances under which information may be released to law enforcement and the elements of information that may be released.

**CRITICAL EDUCATION POINTS**

Generally, the disclosure of Protected Health Information (PHI) to law enforcement or under state / federal law without a patient authorization is limited to the following:

- To comply with legal processes (e.g., subpoena, court order, warrant) and mandated reporting, such as:
  - To report certain crimes on the premises
  - To correctional institutions regarding inmates

Refer to Health Information Department: Requests from law enforcement or for legal processes should be referred to the Health Information Department whenever possible. In emergency situations, clinical staff may disclose non-medical PHI upon inquiry about a specific patient. Disclosure is limited to certain non-medical information (e.g., name, address, age, sex, general description of the patient’s condition, and nature of injury).

**Request identity and validate authority prior to disclosing information:**

In all circumstances of disclosure, the requestor’s identity and authority must be validated and documented.

- **Judicial or Administrative Actions.** Law Enforcement may obtain PHI that is requested pursuant to a valid subpoena, court order or search warrant. Reference specific policies for mandated and required reporting.
- **State and Federal Mandated and Required Reporting.** California Law (CMIA) is not as broad as HIPAA. Disclosures of medical information to law enforcement are required pursuant to a court order, subpoena or search warrant, and/or if required by other laws. Examples include child abuse, domestic abuse, assault, neglect, subpoena, and summons. Health care providers are required to report certain types of wounds and physical injuries, such as gunshot, stabbing, and burns, subject to applicable laws. Reference specific policies for mandated and required reporting.
- **Disclosure of PHI to Law Enforcement -- for Suspected Felon. Location & Identification Information:** In response to an inquiry regarding a specific named patient, in the absence of a subpoena, court order or warrant, California Law (CMIA) limits the disclosure to non-medical information, e.g., suspect’s name, address, age, and sex; a general description of the patient's condition (i.e., fair, stable, critical), treatment and the nature of the injury, burn, poisoning, or other condition. Note: Do not disclose PHI related to the individual’s DNA or DNA analysis, dental records or typing, samples or analysis of body fluids or tissues.
- **Disclosure of PHI to Law Enforcement -- For Victims of Crime.** Disclosure of PHI must be in the best interest of the individual in the professional judgment of the provider and limited to non-medical information. For decedent-victims: Report the suspicion that death involved criminal conduct.
- **Reporting Crime to Law Enforcement – Criminal Conduct on the Premises.** If there is a good-faith belief, that an individual committed a criminal act on the premises of UC_HS, PHI regarding that individual may be disclosed to law enforcement. The PHI disclosure is limited to non-medical information, e.g., nature of crime, location of victim and/or suspected felon, identity, location and description of suspect. Also reference specific policies for mandated and required reporting.
- **Testing for Drug or Alcohol Content.** Law enforcement may obtain drug or alcohol testing information about a patient only if the patient is in the custody of law enforcement and law enforcement requests the test(s).
- **Permitted Disclosures to Correctional Institution - No Authorization Required.** PHI disclosure to a correctional institution or a law enforcement official having lawful custody of an inmate is permitted, if the correctional institution / law enforcement official represents that the PHI is necessary for:
  - The provision of health care to such individuals
  - The health and safety of such individual, other inmates, or others at the correctional institution (e.g., officers, employees, persons responsible for transporting / transferring inmates)
  - You may reasonably rely on the representation of such public officials for the authority to release PHI

**Document disclosures:** These types of disclosures must be documented in order to be included in an accounting of disclosures if requested by the patient. Documentation may be made on a required reporting form if available, i.e., assault, abuse required forms or may be documented on a “Report of PHI Disclosure Form” or other disclosure accounting system. Place copies of required reporting form or the Report of PHI Disclosure form in the medical record or forward to the Health Information Department. [Department specific procedure]
Title: Health Information: Request for Accounting of Disclosures of PHI

**SUMMARY**

One of the new rights established in the Privacy Regulations is the patient's right to obtain an accounting of disclosures made of his/her health information starting April 14, 2003. The accounting may include up to a 6-year period, and generally includes disclosures after 4/14/03 that the patient may not have been aware of that were made of their PHI, e.g., public health disclosures. This policy establishes procedures for how patients may obtain an accounting of disclosures as well as staff documentation procedures of disclosures that must be included in the accounting.

**CRITICAL EDUCATION POINTS**

- The Notice of Privacy Practices informs patients of their right to obtain an accounting of disclosures of their health information. Patients are informed that they must submit a request in writing to the Health Information Department.

- The Patient must be provided with the accounting of disclosures within 60 days of the request. If the accounting cannot be completed within that time frame, the response may be extended for an additional 30 days if the patient has been notified of the reason for the delay and the expected time frame in which the accounting will be ready.

- An accounting need not be made for all disclosures of a patient's PHI. Disclosures that are made for treatment, payment and health care operations or authorized by the patient are not included, or disclosures made prior to April 14, 2003. Generally, disclosures required by law and regulations are included in the accounting. Examples of these types of disclosures include:
  - Disclosures required by law (unless accounting is prohibited by law or suspended)
  - Abuse, assault, domestic violence reporting (check with your supervisor)
  - Judicial and administrative proceedings (unless prohibited by law)
  - Public health activities
  - Organ and tissue donation
  - Certain disclosures for research purposes (e.g., IRB Waiver of Authorizations)

Any UC_HS employee that discloses PHI for the purposes identified above must document such disclosures and forward the information to Health Information for accounting purposes or document the disclosure in the on-line system, if available at the facility.

- **Documentation may be done in one of three ways:** [Facility specific procedure]
  1. Complete a "Report of PHI Disclosure". Include the form in the medical record or forward it to Health Information. The form may be used in circumstances such as verbal disclosures to law enforcement, or when there is mandated reporting and standard reporting forms are unavailable.
  2. Copy of a standard reporting form is included in the medical record. Examples include, assault, abuse, neglect reporting. These forms are completed by the individual making the disclosure and are copied to the medical record.
  3. Maintaining a database of individuals whose information has been disclosed outside of UC. Examples include infection control reporting and lab reporting of infectious disease, or a database of research protocols where patient information may have been viewed through a waived authorization.

- **Elements of each disclosure required in the accounting are:**
  - Date of disclosure
  - Name (and address if known) of the entity or person who received the PHI
  - Brief description describing the PHI disclosed
  - Brief statement describing the purpose of the disclosure of PHI (basis for the disclosure)

- **Responding to Requests for an Accounting:** When the UC_HS Health Information Department receives a request for an accounting, staff will review the entire medical record and/or available database(s), i.e., infection control and IRB to compile a log of all disclosures required in the accounting. If you are unsure as to whether a disclosure is required to be accounted for, complete the Report of PHI Disclosure, the Health Information Department will determine on a case-by case basis whether the disclosure must be included in the accounting. [Facility specific procedure]
**Title:** Health Information: Request for an Amendment or Addendum of PHI

**SUMMARY**

Under California law and the federal Privacy Regulations, patients have the right to request an amendment or an addendum to their health information if they believe their information is inaccurate or incorrect or incomplete. This policy establishes procedures for the patient request to amend or addend their health information.

**CRITICAL EDUCATION POINTS**

Privacy regulations provide patients the right to request amendments to their protected health information (PHI). For example, a patient may ask to change an entry of incorrect, incomplete, or outdated information about them such as name, birth date, or admission date. Or, the patient may ask to amend medical, diagnostic, or treatment information such as progress notes and test results. They also may request the addition of a written addendum to their health information.

- The Notice of Privacy Practices provided during admission/registration informs the patient of their right to submit a written request to amend their health information.

- Refer patients who desire to amend their health information to the Health Information Department.

- Patients must submit their request to the Health Information Management Services department. The request must:
  - Be submitted in writing, (Health Information Management Services will provide a form)
  - Be limited to 250 words, or less, if it is a written addendum
  - Include a reason for the request
  - Identify others who need the amendment
  - All communication of corrections, denials and rebuttals should also be included in future disclosures

- **Amendments.** The Health Information Management Services department must act on the request to amend a record within 60 days of receipt, or may obtain a one-time 30-day extension for responding to the patient’s request provided that they meet the requirements necessary for the extension.

- Health Information, the physician, and/or Risk Management will review amendment requests as appropriate and determine:
  - The impact on the patient’s care and whether the amendment will be accepted in whole or in part
  - Identity of any other entities that may rely on this amended information, and
  - Provide a recommendation for agreement or denial of the amendment.

- If there is agreement for the amendment, Health Information Management Services will include the amendment in the patient’s health record and if necessary make corrections.

- The amendment becomes a permanent part of the medical record and is included with any future third party disclosures. If the amendment is denied, the reason for denial will be documented and forwarded to the patient. Examples of denials include:
  - PHI was not created by the organization
  - PHI is not part of the patient’s medical record
  - The PHI in question is not available to the patient for inspection
  - PHI is accurate and complete as stated

- **Addendums.** Requests to append a written addendum must be accepted subject to a maximum length of 250 words per incorrect entry Health Information Management Services will be responsible for providing a written notice to the patient and continued communication and correspondence as necessary.
HIPAA PRIVACY - POLICY SUMMARY SHEET - #9

Title: Research: Access, Use & Disclosure of PHI

SUMMARY

Protected Health Information (PHI) may be used or disclosed to UC researchers and for UC health care operations under these conditions only: (1) Patient's authorization; (2) IRB waiver of authorization; (3) Limited Data Set and a Data Use Agreement; or (4) De-identification of the data; (5) Deceased patient; or (6) Work preparatory to research with an IRB waiver of authorization. Prospective clinical research is subject to these conditions. The Informed Consent for Clinical Studies can be combined with the Authorization for use of PHI. The UC Notice of Privacy Practices permits these practices. PHI may also be disclosed by workforce to carry out obligatory notification to the FDA of adverse events, to enable product recalls, to track products or to conduct post-marketing surveillance. The patient’s authorization is not required for disclosure of PHI for these obligatory notifications.

CRITICAL EDUCATION POINTS

Requests to access, use or disclose PHI for research purposes fall under general categories:

- **USE & DISCLOSURE - with Patient's Authorization** (or patient's consent to participate in a clinical study):
  - Disclosure: May be combined with other consent or authorization
  - Minimum necessary standard applies
  - No accounting of disclosure required

- **USE & DISCLOSURE - with a HIPAA Compliant Authorization** from the patient
  - During transition period from 4/14/03 until the annual study review by the IRB, subjects newly enrolled into existing studies after 4/14/03 will require additional “HIPAA compliant authorization language” (available on irb.ucsd.edu website);
  - Minimum necessary standard applies
  - No accounting of disclosure required

- **USE & DISCLOSURE - with an IRB “Waiver of Authorization”**
  - Clinical trial investigator obtains a “Waiver of Authorization” from the IRB
  - Minimum necessary standard applies
  - Requires accounting of disclosure
  - Requires special processes for reporting disclosures for research studies with >50 patients enrolled

- **USE & DISCLOSURE - with a Limited Data Set and a Data Use Agreement**
  - Requires IRB approved research plan
  - Limited data set contains only 5-digit zip codes and dates, e.g., dates of admission and discharge, dates of service, date of birth or age, and date of death.
  - Data Use Agreement: specific form with requestor’s agreement: not to re-identify, not to re-disclose, and to maintain confidentiality of data for the stated purpose
  - Limited data sets are restricted to 3 purposes: research, public health reporting, UC’s own health care operations.
  - No authorization is required
  - No accounting of disclosure required

- **USE & DISCLOSURE - with De-identification of Data**
  - Removal of 18 protected health identifiers (at least). De-identified data is no longer PHI.
  - No authorization required
  - No accounting of disclosures required
  - De-identification by statistically valid methodology

- **USE & DISCLOSURE - for Decedents**
  - No authorization or waiver required; however the UC IRBs may choose to review decedent research requests
  - IRB approval is required if the request involves research with decedent information created by California state agencies;
  - Accounting of disclosure is required

- **USE & DISCLOSURE - for Research Registries and Databases**
  - Requires individual’s authorization to be part of an on-going registry or database, unless previous permission was granted;
  - Authorization for registry may be combined with subject consent;
  - Requires IRB approval to access registry / databases for new studies
Title: De-Identifying & Re-identifying Data that Contains PHI; Limited Data Sets; Data Use Agreements

SUMMARY

It is the policy of (UC_HS) to safeguard the confidentiality and security of information, including patient protected health information (PHI). Only health information that “identifies” an individual is subject to the HIPAA privacy standards. The HIPAA regulations also allow the use and disclosure of PHI contained in a “limited data set” for research, health care operations and public health purposes. UC_HS will, from time to time, use de-identified data and limited data sets for various purposes. In doing so, UC_HS will insure that the appropriate administrative and technical processes are in place to properly de-identify PHI, as well as to re-identify PHI when required. The disclosures of de-identified information and/or limited data sets do not need to be part of an accounting of disclosures requested by an individual.

CRITICAL EDUCATION POINTS

- De-Identification
  - Removal of at least 18 protected health information (PHI) identifiers (see Exhibit A)
  - De-identified information is no longer considered PHI and may be freely used
  - A Business Associate may receive PHI to de-identify for UC’s or the BA’s purposes (if permitted to do so by the business associate agreement)

- Re-Identification
  - HIPAA privacy standards allow information that has been de-identified, to be re-identified if: The means to re-identify such as a code may not be derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and the covered entity does not use or disclose the means of re-identification for any other purpose and does not disclose the mechanism for re-identification.
  - Re-identification is sometimes necessary as when a product recall is issued by the FDA and participants in a research study need to be contacted.

- Limited Data Set (LDS)
  - Removal of all direct identifiers (see Exhibit A)
  - Include 5-digit zip codes and dates, e.g., date of birth or age, date of death, date of admission, date of discharge, dates of service
  - May be used for 3 purposes only: research; healthcare operations; and public health, e.g., in conjunction with disease registries not covered by law or regulation.
  - Requires a data use agreement between the requester and the UC data steward with assurances not to re-disclose or to re-identify or contact the patients.
  - Limited data sets are not required to be included in the log of accounting of disclosures

- Data Use Agreement
  - Describes the permitted uses and disclosures by the recipient of LDS
  - Contains assurances of: safeguards, no re-disclosure, no re-identification; subcontractors are obligated by the terms
**HIPAA Fact Sheet - #11: De-Identification of PHI vs. Limited Data Sets**

**De-Identification of Information**

**List of 18 Protected Health Information (PHI) Data Elements**

The following 18 identifiers regarding the individual, relatives, or household members are regarded as “protected health information” or PHI:

Reference: HIPAA 45 CFR §164.502 d; 164.514

**Limited Data Set (LDS)**

List of Data Elements that may be included in a LDS for limited purposes only: research, health care operations and public health disclosures (e.g., disease registries).

The shaded columns illustrate what must be excluded (removed) from PHI to fully de-identify the data set.

Reference: HIPAA 45 CFR §164.514 e (August 2002)

<table>
<thead>
<tr>
<th>DE-IDENTIFIED PROTECTED HEALTH INFORMATION (PHI)</th>
<th>LIMITED DATA SET</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EXCLUDES</strong></td>
<td><strong>EXCLUDES</strong></td>
</tr>
<tr>
<td>2. Street Address, City, State, Zip code *</td>
<td>8. Medical record numbers</td>
</tr>
<tr>
<td>3. All Dates: Age &lt;90: All elements of dates, except year; Age &gt;89: All elements of dates including year</td>
<td>9. Health plan beneficiary numbers</td>
</tr>
<tr>
<td>4. Telephone numbers</td>
<td>10. Account numbers</td>
</tr>
<tr>
<td>5. Fax numbers</td>
<td>11. Certificate license numbers</td>
</tr>
<tr>
<td>6. Electronic mail addresses</td>
<td>12. Vehicle identifiers and license numbers</td>
</tr>
<tr>
<td></td>
<td>3. Any other unique identifying number, characteristic or code</td>
</tr>
</tbody>
</table>

* MNS = Minimum necessary standard
Title: Uses & Disclosures of PHI for Fundraising / External Relations, Media / Public Information, Marketing

**SUMMARY**

**External Relations / Fundraising.** Access to protected health information (PHI) for external relations activities / fundraising is restricted as defined in the Notice of Privacy Practices. A covered entity may use or disclose PHI for the purpose of external relations for its own benefit without authorization, if it provides only demographic information related to the individual and dates of health care provided to the individual and incorporates appropriate safeguards. Diagnosis and/or disease may **not** be supplied. Patients receiving any solicitation for external relations purposes must be given an opportunity to be excluded (opt-out) from further contacts.

**Marketing.** Under HIPAA regulations, marketing is defined as “making a communication about a product or service that encourages the recipients of the communication to purchase or use the product or service.” In general, marketing communications using protected health information (PHI) require a prior written authorization. A patient authorization is required for use or disclosure of any PHI for purposes of marketing, unless the activity is provided face-to-face by the patient’s provider. Because of the complexity of these regulations, faculty and staff should consult with the UC External Relations Staff, Marketing or the UC Privacy Officer before using PHI in any marketing activities.

**CRITICAL EDUCATION POINTS**

- **Fundraising for UC**
  - Minimum necessary for fundraising is: demographic data and dates of service only;
  - Demographic data for this purpose is only the: individual’s name, date of birth, gender, ethnicity, insurance status, address and other contact information.
  - Diagnosis data, disease may **NOT** be released. If the treating provider(s) name/department could identify the diagnosis/disease, then that information must also be restricted.
  - All communications must contain instructions on how to “opt-out” from future contacts
  - Fundraising staff and/or public relations staff of UC_HS may assist the provider in fundraising by preparing mailings, phone calls or other contact names.
  - A patient authorization is required for disclosure of more than the minimum necessary PHI as described above

- **Marketing**
  - Minimum necessary standard applies to all requests for PHI for marketing
  - Permitted marketing communications include — (1) information provided for the purpose of furthering or managing the treatment of an individual, such as directing or recommending to that individual alternative treatments, therapies, health care providers or settings of care; (2) information about entities participating in a provider network or health plan, including the services offered by those providers; or the benefits covered by a health plan, including replacements to and enhancements for coverage under the plan; (3) face-to-face communications made by a covered entity to an individual; or (4) promotional gifts of nominal value provided by the covered entity.
  - All other types of marketing communications requires a prior authorization
  - Refer initial marketing plan to the Privacy Officer to evaluate whether the activity is permissible without a patient authorization
  - PHI may not be disclosed or sold to any vendor to market its own product / service.

- **External Relations / Public Information / Media Requests**
  - Media requests for stories: Refer requests from media to the UC __ Public Information Office. The public information office will contact the primary provider, who is responsible for contacting the patient. UC must obtain a written authorization from the individual prior to any contact.
  - Media requests for information regarding a specific named patient. Information that may be disclosed is limited to facility directory information, e.g., general condition: stable, guarded, and critical.
  - Requests for Treatment / Disease Specific Information / PHI: Requires a valid patient authorization
  - Requests for Photos / Images / Video: Requires a separate authorization
  - Databases for future media contacts: Requires patient’s authorization to be included in the listing.
HIPAA PRIVACY - POLICY SUMMARY - #13

Title: Personal Representatives

SUMMARY
Patients may designate a personal representative to act on their behalf. The personal representative is someone who is legally authorized to make healthcare decisions about the patient, including signing authorizations for disclosure of PHI, requesting accountings of disclosures and other requests on behalf of the patient. Usually the personal representative for an unemancipated minor will be the parent or legal guardian. There may be circumstances in which treating the personal representative as if he/she were the patient may not be appropriate. In situations of alleged abuse, domestic violence, or neglect, it may be appropriate to deny or limit access by the personal representative in order to protect the patient’s best interests.

CRITICAL EDUCATION POINTS

Minors
- All persons under 18 years of age with exceptions for minors who are: married or previously married; emancipated; or on active duty in the Armed Forces
- Parent, guardian, or other person acting in loco parentis usually has the authority to make healthcare decisions about the unemancipated minor patient
- EXCEPTIONS APPLY when a minor …
  - Is a possible victim of violence, abuse or neglect
  - Is legally an emancipated minor
  - Is a minor is making decisions about sensitive services, e.g., reproductive healthcare, communicable disease, or substance abuse counseling

Decisionally Incapacitated Adults
- A patient is a decisionally incapacitated to make a healthcare decision if he or she is unable to understand their medical condition, the risks and benefits of recommended treatments and available alternatives.
- The personal representative will be a legal guardian or conservator
- Use professional judgment to determine (spouse, children, etc.)

Decedents
- The executor or administrator of the decedent’s estate may authorize the release of the patient’s PHI
- Copies of the executor or administrator’s appointment documents must accompany the authorization
- If there is no executor or administrator, the patient’s next of kin has the authority

Disclosures of PHI to the Personal Representative
- Use professional judgment and experience to determine what PHI should be disclosed to a personal representative
- Patient’s objections and restrictions must be honored
- Minimum necessary standard applies to disclosure of information to:
  - Locate or identify a family member, relative or other individual involved in the patient’s care
  - PHI relevant to the representatives involvement in the care, for example, limited to pick up of prescriptions
- If the request to disclose the PHI to the personal representative is by phone, establish a verification process to confirm identify of the caller. Example: Request that the caller provide the patient’s medical record or account number or home phone number and date of birth; or use a call back procedure
- If in doubt, do not disclose any information and request assistance from your supervisor, the Privacy Officer, and/or Risk Management
- For inquiries regarding inpatients, check the facility directory to identify “no disclosure” patients first!
**Under HIPAA, a vendor or third-party entity that handles PHI on behalf of UC is our “business associate” and we are required to have them agree to comply with the Federal HIPAA privacy and security requirements through a contract agreement or amendment. This requirement applies to companies or persons who conduct, for example, the following activities or functions, such as:**

1. Claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and re-pricing; or
2. Legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services, to or for UC__.

This is not an all-inclusive list. In these circumstances, refer the purchase/contract or agreement request to the UC__ Healthcare Purchasing Director (____-_____) or the Campus Purchasing Director (________) to implement a “business associate agreement” with the vendor or third-party entity. The agreement can be handled as an addendum for existing contracts. Call the UC Purchasing Director for clarification if you are unsure about whether the third party vendor is a Business Associate.

### CRITICAL EDUCATION POINTS

- **Why are Business Associate Agreements needed?**
  - DHHS created the “Business Associate” concept to extend the accountability for protecting health information (PHI) beyond a healthcare provider, health plan or clearing house.
  - HIPAA Privacy regulations will affect many businesses that have a relationship with a covered entity. These organizations will need to execute a legally binding Business Associate Agreement, and in many cases, possibly change the way they conduct business.

- **A business associate relationship exists when an entity or an individual …**
  - Performs or assists in the performance of a function or activity on behalf of UC or provides services to UC, and
  - The service provided involves the use or disclosure of protected health information (PHI), and
  - Personnel performing the function, activity or service are not acting in the capacity of a member of the workforce

- **Five exceptions that do not require a business associate agreement:**
  - Treatment
  - Disclosures for financial transactions, e.g., a bank receives CE’s credit card transactions, cashes checks for payment of healthcare services
  - Couriers of closed or sealed materials, e.g., U.S. Postal carriers, FEDEX, UPS, or other mail/messenger services transporting PHI in a closed or sealed container, package or envelope which conceals the contents
  - Disclosures between group health plan and plan sponsor
  - Disclosures between organized health care arrangements, e.g., network of an IPA

- **You do not need a Business Associate Agreement for…**
  - Treatment, Payment, or Healthcare Operations (TPO) disclosures between UC and your healthcare employees and UC healthcare trainees.
  - Disclosures to Hospitals, Healthcare Providers, Health Plans or Healthcare Clearinghouses for TPO
  - Disclosures to other contracted individuals, and volunteers, IF they function as a member of your workforce and receive privacy training

- **General Rule for Business Associates:**
  - If the covered entity (i.e., UC) cannot use or disclose the PHI, then a business associate cannot either!
  - Same restrictions apply to the business associates’ subcontractors and agents
HIPAA’s privacy rule states that providers may charge a reasonable, cost-based fee for providing copies of PHI including the costs of copying (such as supplies and labor), postage (if the individual requested that the PHI be mailed) and a cost for the preparation of any summary or explanation, if agreed to in advance. Providers may also establish reasonable conditions, including a reasonable deposit fee, to ensure the return of original x-rays.

California law is more specific and allows the providers to charge fees to patients as follows (Year: 2003):

- Photocopy Fee = 25 cents per page
- Clerical Costs/Hour = $15/hour (Clerical costs incurred in locating and making records available may not be charged to patients after April 14, 2003, but may be billed to others.)
- Microfilm copies = 50 cents per page
- X-Ray Film Duplication = $5.00 per x-ray film
- If a summary is provided, a reasonable fee may be charged based on actual time and cost for the preparation of the summary with the patient’s agreement in advance.

The fee allowed by California law for clerical costs incurred in locating and making the record available is not allowed under HIPAA, and may not be billed to patients after April 14, 2003. The fee may still be billed to other providers, attorneys, insurance companies, etc., if the provider so desires. The special fee structure applies to requests for PHI from attorneys not representing the patient, insurance companies, disability determinations, subpoenas, etc.

### Waiver of Copy Fees for Patients with Economic Need.

An individual who does not have the ability to pay may be given copies of records in the designated record set without charge upon providing proof of economic need. Such proof may include, but is not limited to participation in the state Medi-Cal or charity care programs.

A patient, former patient or the patient’s representative shall be entitled to a copy, at no charge, of the relevant portions of the patient’s records, upon presenting to the provider a written request and proof that the records are needed to support an appeal regarding eligibility for public benefit program (e.g., Medi-Cal, social security disability insurance benefits, and a Supplementary Program for the Aged, Blind and Disabled (SSI/SSP) benefits). [Cal. Health & Safety Code § 123110 d]

### Timely Response Required for Record Requests

Upon written request, an adult patient or the patient's representative is entitled to inspect and obtain a copy of his/her medical records. A patient is allowed to inspect her records during business hours within five working days after the provider receives the written request. A provider may require the patient to pay reasonable clerical and copying fees, not to exceed twenty-five ($0.25) cents per page, or fifty ($0.50) cents per page of microfilm. The copies should be sent by the health care provider within fifteen days after receiving the written request. The provider may also require reasonable verification of identity prior to permitting inspection or copying of the records.

Rather than provide direct access to the patient's medical records, a health care provider may provide a summary of the records if the patient agrees. This information must contain specifics about each injury, illness or episode including the patient's chief complaint, the diagnosis, treatment plan, prognosis, pertinent test results and discharge summaries. A provider can charge no more than a reasonable fee based upon actual time and cost for preparation of the summary.
HIPAA Fact Sheet - #16: Security Standards

The final security standards for HIPAA were published by HHS on February 20, 2003. Under this rule, health insurers, certain healthcare providers, and health care clearinghouses must establish procedures and mechanisms to protect the confidentiality, integrity and availability of electronic protected health information. The rule requires covered entities to implement administrative, physical, and technical safeguards to protect electronic PHI that they receive, store, or transmit. Most covered entities will have two full years – until April 21, 2005 – to comply with the standards; small health plans will have an additional year to comply.

Key Features of the Final Security Rule

The security standards are:

- **Scalable** – Covered entities may take into account their size, complexity, capabilities, costs of complying with the standards, and the potential risks to their PHI.

- **Technology neutral** – The standards do not specify any particular technology. They outline what must be done, not how to do it.

- **Designed to protect electronic data at rest and in transit through:**
  - **Administrative safeguards** – Management of the selection and execution of security measures
  - **Physical safeguards** – protection of electronic systems and related buildings and equipment from environmental hazards and unauthorized intrusion.
  - **Technical safeguards** – Automated processes to protect data and control access to it.

The Security Standards use many of the same terms and definitions as the Privacy Standards. Reference: [http://www.cms.hhs.gov/hipaaa/hipaa2](http://www.cms.hhs.gov/hipaaa/hipaa2)

Reasonable Safeguards that should be taken with electronic information now include:

- Do not share your computer passwords with anyone
- Do not leave your passwords posted or attached to your computer or easily visible on your desk
- Make sure computer screens are not visible to passersby
- Use Privacy screens whenever possible
- Log off your computer when you are done, or if you walk away from the computer for a period of time
- If possible, use automatic time-outs or screen savers to protect the information from being easily visible
- Do not allow any individual to use your terminal after you have signed in. Any information changed/altered or accessed can be traced back to your login, and you will be held responsible for the PHI that was altered or accessed
Health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a transaction for which the Secretary of DHHS has adopted a standard will be required to use the adopted standards. The standard transactions for administrative and financial health care transactions are:

1. Health claims and equivalent encounter information (e.g., CPT, ICD9, HCPCS codes)
2. Enrollment and disenrollment in a health plan
3. Eligibility for a health plan
4. Health care payment and remittance advice
5. Health plan premium payments
6. Health claim status
7. Referral certification and authorization
8. Coordination of benefits.

Congress and the health care industry have agreed that standards for the electronic exchange of administrative and financial health care transactions are needed to improve the efficiency and effectiveness of the health care system. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of Health and Human Services to adopt such standards.

With a national standard for electronic claims and other transactions, health care providers will be able to submit the same transaction to any health plan in the United States and the health plan must accept it. Health plans will be able to send standard electronic transactions such as remittance advices and referral authorizations to health care providers. These national standards will make electronic data interchange a viable and preferable alternative to paper processing for providers and health plans alike.

Standards for the first report of injury and claims attachments (also required by HIPAA) will be adopted at a later date.

What standards were chosen?
ANSI ASC X12N standards, Version 4010, were chosen for all of the transactions except retail pharmacy transactions. The choice for the retail pharmacy transactions was the standard maintained by the NCPDP because it is already in widespread use. The NCPDP Telecommunications Standard Format Version 5.1 and equivalent NCPDP Batch Standard Version 1.0 have been adopted in this rule (health plans will be required to support one of these two NCPDP formats).

Where can I obtain implementation guides for the standards?
The implementation guides for the ASC X12N standards may be obtained from the Washington Publishing Company, 806 W. Diamond Ave., Suite 400, Gaithersburg, MD, 20878; telephone: 301-949-9740; FAX: 301-949-9742. These guides are also available at no cost through the Washington Publishing Company on the Internet at http://www.wpc-edi.com/hipaa/.

The implementation guide for retail pharmacy standards is available from the National Council for Prescription Drug Programs, 4201 North 24th Street, Suite 365, Phoenix, AZ, 85016; telephone: 602-957-9105; FAX: 602-955-0749. It is also available from the NCPDP’s website at http://www.ncpdp.org.

How will the standards affect data stored in my system?
The transaction standards will apply only to electronic data interchange (EDI) -- when data are transmitted electronically between health care providers and health plans as part of a standard transaction. Data may be stored in any format as long as it can be translated into the standard transaction when required. Security standards, on the other hand, will apply to all health care information.
REFERENCES

Web Links For HIPAA Privacy, Security, Transactions and Code Sets

1. Office for Civil Rights (OCR) - HIPAA
   Medical Privacy - National Standards to Protect the Privacy of Personal Health Information
   OCR Guidance Explaining Significant Aspects of the Privacy Rule - December 4, 2002
   http://www.hhs.gov/ocr/hipaa/privacy.html

2. Center for Medicare and Medicaid Services (CMS) – HIPAA
   The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
   http://www.cms.gov/hipaa/

3. Department of Health & Human Services (DHHS)
   Final Security Rule
   Published as a Final Rule on February 20, 2003. Compliance required by April 21, 2005)
   Standards for Electronic Transactions & Code Sets
   Published as a Final Rule on August 17, 2000, Compliance required by October 16, 2003
   http://www.wedi.org/snip/public/articles/index~15.htm

4. HIPAA.ORG -- Website with many helpful links
   http://www.hipaa.org/

5. State of California - Office for HIPAA Implementation (CalOHI)
   http://www.ohi.ca.gov/state/calohi/ohiHome.jsp

6. California HealthCare Foundation – HIPAA
   http://www.chcf.org/

7. University of California – HIPAA  <website coming soon>